(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 31 047 A 1**

(51) Int. Cl.[7]:
G 01 R 31/3183
G 06 F 11/00
G 06 F 12/14

(21) Aktenzeichen: 199 31 047.5
(22) Anmeldetag: 6. 7. 1999
(43) Offenlegungstag: 13. 1. 2000

DE 199 31 047 A 1

(30) Unionspriorität:
98/08846 09. 07. 1998 FR

(71) Anmelder:
Schlumberger Systemes, Montrouge, FR

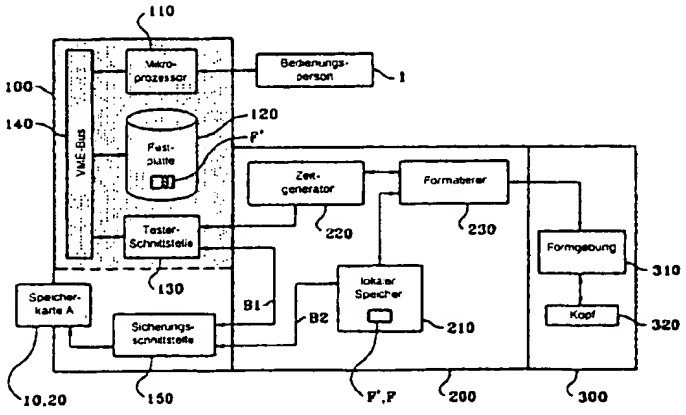
(74) Vertreter:
Sparing . Röhl . Henseler, 40237 Düsseldorf

(72) Erfinder:
Gazounaud, Yann, Saint Just, Saint Rambert, FR;
Wach, Max, Saint Etienee, FR

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zum Sichern von Daten in einer Maschine zum Testen elektronischer Bauteile

(57) Ein Verfahren zum Sichern von Daten in einer Maschine zum Testen elektronischer Bauteile, die eine Zentraleinheit (100), die mit einem Speichermittel (120) versehen ist, und einen über einen Übertragungsbus (B1, B2) mit dem Speichermittel (120) verbundenen lokalen Speicher (210) enthält. Das Verfahren umfaßt die folgenden Schritte: Herstellen wenigstens einer Datei (F) von Testvektoren, Verschlüsseln der in der Datei (F) von Testvektoren enthaltenen Daten mit Hilfe eines Verschlüsselungs-/Entschlüsselungsmittels (10), Installieren der verschlüsselten Datei (F') von Testvektoren im Speichermittel (120) der Zentraleinheit, vor jedem Test Laden der verschlüsselten Datei (F') von Testvektoren in den lokalen Speicher (210) über den Übertragungsbus (B1, B2), Entschlüsseln der verschlüsselten Daten (F') von Testvektoren mit Hilfe des Verschlüsselungs-/Entschlüsselungsmittels (10) und anschließend Ausführen des Tests.



DE 199 31 047 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zum Sichern von Daten in einer Maschine zum Testen elektronischer Bauteile nach dem Oberbegriff des Anspruchs 1.

Im allgemeinen ist eine Maschine zum Testen elektronischer Bauteile im wesentlichen aus drei Elementen gebildet:

- aus einer Zentraleinheit (CPU), die insbesondere mit einem Speichermittel wie etwa einer Festplatte versehen ist, auf der wenigstens eine Datei für den auszuführenden Test installiert ist. Diese Zentraleinheit ist ein Rechner, der einer Bedienungsperson ermöglicht, den Test zu starten, bestimmte Parameter während der Ausführung zu überwachen und die Daten am Ende des Tests einzusammeln. Die Testdateien enthalten unter anderem eine Wahrheitstabelle, wovon jede Spalte einem Anschluß der getesteten Bauteile entspricht und wovon jede Zeile, die auch Vektor genannt wird, eine Konfiguration der logischen Signale 0 oder 1 definiert, die entweder Erregungssignale sind, die an bestimmte Anschlüsse anzulegen sind, oder Antworten, die auf die an andere Anschlüsse angelegten Erregungssignale erwartet werden;
- aus einer Testelektronik, die mit der Zentraleinheit über eine Tester-Schnittstelle verbunden ist, die sich zwischen dem Bus der Zentraleinheit und einem Übertragungsbus der Testelektronik befindet und über die die Dateien von Testvektoren vor ihrer Ausführung von der Festplatte der Zentraleinheit zu einem lokalen Speicher der Testelektronik transportiert werden. Diese Transportoperation von Dateien von Testvektoren ist deshalb notwendig, weil ein Test, der direkt anhand der auf der Festplatte gespeicherten Dateien ausgeführt würde, wegen der Zeit zum Lesen von der Festplatte sowie wegen der Zeit zum Übertragen der Dateien zwischen der Festplatte und der Testelektronik über die Tester-Schnittstelle viel zu lang dauern würde. Die Testelektronik enthält außerdem einen Zeitgenerator, der dazu vorgesehen ist, Zeitpunkte zu liefern, die in einer zeitlichen Folge von Ereignissen angeordnet sind. Ein Formatierer hat die Aufgabe, die Vektoren der Wahrheitstabelle in der vom Zeitgenerator empfangenen zeitlichen Folge in der Weise zu organisieren, daß ein Zug logischer Signale gebildet wird, der mit den aufeinanderfolgenden Operationen in Übereinstimmung ist, bevor sie im Verlauf des Tests ausgeführt werden;
- aus einem Arbeitskopf, in dem die zu testenden elektronischen Bauteile angeordnet sind und der einen elektronischen Anschluß enthält, dessen Funktion darin besteht, die logischen Erregungssignale in Abhängigkeit von der Technologie und der Logik, die von den Bauteilen verwendet werden, in analoge Form zu bringen und umgekehrt die Antworten der Bauteile auf die angelegten Erregungssignale in logische Form zu bringen.

Derzeit sind die Dateien von Testvektoren auf der Festplatte der Zentraleinheit unverschlüsselt installiert. Auf ihren Inhalt, insbesondere auf die Testvektoren, kann daher vom Rechner der Testmaschine einfach zugegriffen werden, so daß der Inhalt auf jeden beliebigen Träger, insbesondere Disketten, kopiert werden kann. Außerdem ist im Betrieb der Maschine ein "Austest"-Modus zum Lesen oder Modifizieren des lokalen Speichers nach seinem Laden vorgesehen. In diesem besonderen Modus ist es daher möglich, auf die in den lokalen Speicher geladenen Dateien und von hier aus auf die Testvektoren zuzugreifen.

Nun enthalten die Testvektoren sensible Daten wie etwa die Codes von Bankkarten, eingebettete Software wie etwa Spielesoftware, die durch das Recht des Autors geschützt ist, oder aber Kennwörter, die den Zugang zu Komponenten ermöglichen, um Software, die während des Tests implantiert wird, zu lesen.

Aufgabe der Erfindung ist es, ein Verfahren nach dem Oberbegriff des Anspruchs 1 zu schaffen, mit dem der Zugriff auf Dateien von Testvektoren während der verschiedenen Phasen seines Ablaufs begrenzt und kontrolliert werden kann.

Diese Aufgabe wird entsprechend dem kennzeichnenden Teil des Anspruchs 1 gelöst.

Weitere Ausgestaltungen der Erfindung sind der nachfolgenden Beschreibung und den Unteransprüchen zu entnehmen.

Ein derartiges Sicherungsverfahren ermöglicht somit, den Zugriff auf sensible Daten zu verhindern, wenn die Testvektor-Datei in dem Speichermittel, insbesondere der Festplatte der Zentraleinheit installiert ist.

Wie jedoch weiter oben erwähnt worden ist, ist es selbst nach dem Laden der Testvektordatei möglich, auf den lokalen Speicher und daher auf die nichtverschlüsselten sensiblen Daten zuzugreifen, wenn der Lese- oder Modifikationsmodus, d. h. "Austest"-Modus, verwendet wird, der dazu bestimmt ist, der Bedienungsperson zu ermöglichen, bei Auftreten von Fehlern während der Ausführung des Tests einzugreifen. Deshalb ist vorgesehen, daß nach dem Schritt des Entschlüsselns der Zugriff zum Lesen oder Modifizieren des lokalen Speichers untersagt wird. Wenn jedoch gewünscht ist, daß die Bedienungsperson den lokalen Speicher lesen oder modifizieren kann, um beispielsweise bei der Durchprüfung des Programms oder bei der Suche eines Problems im Test eine Korrektur auszuführen, besteht der Vorteil, daß der Zugriff zum Lesen oder Modifizieren des lokalen Speichers bei Angabe einer Zugriffsberechtigung zugelassen wird.

Gemäß einer besonderen Ausführung ist das Verschlüsselungs-/Entschlüsselungsmittel eine elektronische Chipkarte, die einen geheimen Schlüssel und einen Verschlüsselungs-/Entschlüsselungs-Algorithmus enthält. Die somit erhaltene Sicherheit ist sehr hoch, weil einerseits der geheime Schlüssel, der in den Speicher der Karte eingebettet ist, weder der Person, die die sensiblen Daten verschlüsselt, noch der Bedienungsperson bekannt sein kann und weil er andererseits niemals zur Testmaschine übertragen wird, weil die Karte selbst die Entschlüsselung ausführt.

Ebenso kann vorgesehen sein, daß die Zugriffsberechtigung in einer elektronischen Chipkarte enthalten ist, die im allgemeinen von der Verschlüsselungs-/Entschlüsselungskarte verschieden ist, jedoch im "Austest"-Modus mit allen Zugriffsprivilegien versehen ist.

Die Erfindung wird nachstehend anhand eines in den beigefügten Abbildungen dargestellten Ausführungsbeispiels näher erläutert.

Fig. 1 ist ein Blockschaltplan einer Testmaschine, mit der das Sicherungsverfahren ausgeführt werden kann.

Fig. 2 ist ein Blockschaltplan, der die verschiedenen Schritte des Sicherungsverfahrens veranschaulicht.

Die **Fig.** 3a bis 3e sind Blockschaltpläne, die die aufeinanderfolgenden Funktionen der Sicherungsschnittstelle der Testmaschine von **Fig.** 1 veranschaulichen.

In **Fig.** 1 sind in Form von Blockschaltplänen die Hauptelemente einer Testmaschine gezeigt, die bereits im einleitenden Teil dieser Abhandlung erwähnt worden sind. Die Testmaschine enthält eine Zentraleinheit **100**, die von einer Bedienungsperson **1** mittels einer Tastatur und eines Bildschirms gesteuert wird und einen Rechner **110** sowie ein

Speichermittel **120**, hier eine Festplatte, enthält, wobei das Speichermittel **120** dazu vorgesehen ist, die Datei(en) zu empfangen, die die Testvektoren enthält (enthalten), die in einer Wahrheitstabelle angeordnet sind. Für die Bezeichnung einer Datei von Testvektoren wird entweder der Buchstabe F für die unverschlüsselte Datei oder der Buchstabe F' für die verschlüsselte Datei verwendet. Wie in **Fig.** 1 gezeigt ist, ist die Festplatte **120** dazu vorgesehen, die Dateien von Testvektoren in verschlüsselter Form zu speichern.

Die Zentraleinheit **100** enthält außerdem eine Vorrichtung zum Lesen von elektronischen Chipkarten sowie eine Sicherungsschnittstelle **150**, deren Funktionen später beschrieben werden.

Ein VME-Bus **140** der Zentraleinheit **100** ermöglicht die Kommunikation zwischen dem Rechner **110**, der Festplatte **120** und einer Tester-Schnittstelle **130**, die den Zugriff auf eine Testelektronik **200** ermöglicht, die die Einheit bildet, die die Aufgabe hat, sämtliche Testoperationen an den elektronischen Bauteilen auszuführen, die auf einem Arbeitskopf **300** der Maschine angeordnet sind.

Die Testelektronik **200** enthält einen lokalen Speicher **210**, der mit der Tester-Schnittstelle **130** der Zentraleinheit **100** über einen Bus B1, B2 für die Übertragung über die Sicherungsschnittstelle **150** verbunden ist. Der lokale Speicher **210** ist dazu vorgesehen, die Testdateien zu empfangen, deren Vektoren anschließend durch einen Formatierer **230** in einen Zug logischer Signale geformt werden, die durch einen Zeitgenerator **220** in einer zeitlichen Folge angeordnet werden, wobei die logischen Signale anschließend durch eine im Arbeitskopf **300** enthaltene elektronische Formgebungseinheit **310** in geeignete Signale umgesetzt werden, wobei die Bauteile auf dem eigentlichen Kopf **320** angeordnet sind.

Um die in den Vektoren der Testdatei enthaltenen sensiblen Daten zu sichern, wird ein Verfahren vorgeschlagen, das nun mit Bezug auf die **Fig.** 1, 2 und 3 beschrieben wird.

Das Sicherungsverfahren sieht zu einer ersten Zeit vor, daß nach dem Herstellen wenigstens einer Datei F von unverschlüsselten Testvektoren diese Datei wenigstens teilweise durch ein Verschlüsselungs-/Entschlüsselungsmittel verschlüsselt wird, das in der beschriebenen Ausführung eine elektronische Chipkarte **10** ist, die einen geheimen Schlüssel und einen Verschlüsselungs-/Entschlüsselungs-Algorithmus enthält. Die Verschlüsselungsoperation kann in der Testmaschine selbst ausgeführt werden, indem ein Kartenleser verwendet wird, wie in **Fig.** 1 angegeben ist. Sie kann jedoch auch an einem völlig anderen Ort ausgeführt werden, wobei die verschlüsselte Datei F' dann zur Testmaschine geliefert wird und dabei von der Verschlüsselungs-/Entschlüsselungskarte **10** begleitet wird.

Im allgemeinen ist die Verschlüsselung der Testvektoren wesentlich partiell und stützt sich nur auf die sensiblen Daten, die geschützt werden sollen. Dies ist in den **Fig.** 2 und 3 durch die punktierte Zone der Datei F' symbolisch dargestellt.

Nach der Kompilierung wird die verschlüsselte Datei F' auf der Festplatte **120** der Testmaschine installiert. Dann kann insbesondere die Bedienungsperson **1** nicht auf die sensiblen Daten zugreifen, wobei der in **Fig.** 1 grau unterlegte Bereich der Zentraleinheit **100** zu einer vollkommen geschützten Zone wird.

Wenn der Test ausgeführt werden soll, wird aus den weiter oben angegebenen Gründen die verschlüsselte Datei F' der Testvektoren etwa von der Festplatte **120** über den Übertragungsbus B1, B2 an den lokalen Speicher **210** übertragen. Diese Operation entspricht dem Schritt a) von **Fig.** 3, in dessen Verlauf die Sicherungsschnittstelle **150** die Kontinuität zwischen den Abschnitten B1 und B2 des Übertragungsbusses sicherstellt.

Um anschließend den Test ausführen zu können- wird die verschlüsselte Datei F' in der elektronischen Verschlüsselungs-/Entschlüsselungs-Chipkarte **10**, die in das Lesegerät der Testmaschine eingeführt wird, das mit der Sicherungsschnittstelle **150** verbunden ist, entschlüsselt und zum lokalen Speicher **210** zurückgeschickt. Während dieser Entschlüsselungsphase, die im Schritt b) von **Fig.** 3 gezeigt ist, ist nur der Abschnitt B2 des Übertragungsbusses unter der Steuerung der Sicherungsschnittstelle **150** aktiv.

Nach der Entschlüsselung wird für die Verifikation eine Quittierungsnachricht zur Zentraleinheit **100** geschickt, derart, daß die empfangene Quittierung der richtigen Verschlüsselungs-/Entschlüsselungskarte **10** entsprechen muß und daß die entschlüsselte Datei in Ordnung sein muß.

Nach dem Laden der Testvektoren und wie im Schritt c) von **Fig.** 3 gezeigt ist, untersagt die Sicherungsschnittstelle **150** jeden Zugriff auf den lokalen Speicher **210** zum Lesen oder Modifizieren ("Austest"-Modus). Falls sich jedoch ein Eingriff der Bedienungsperson **1** aufgrund einer Anomalie im Ablauf des Tests als notwendig erweist, wäre es möglich, auf den "Austest"-Modus zuzugreifen, um den lokalen Speicher **210** bei Eingabe einer Zugriffsberechtigung, die beispielsweise in einer in das Lesegerät der Testmaschine eingeschobenen elektronischen Chipkarte **20** enthalten ist, zu lesen oder zu modifizieren, wie im Schritt d) von **Fig.** 3 gezeigt ist.

Am Ende des Tests stellt die Sicherungsschnittstelle **150** wieder die Kommunikation über den Übertragungsbus B1, B2 her, nachdem selbstverständlich die Datei F von unverschlüsselten Testvektoren aus dem lokalen Speicher **210** entfernt worden ist.

Patentansprüche

1. Verfahren zum Sichern von Daten in einer Maschine zum Testen elektronischer Bauteile, die eine Zentraleinheit (**100**), die mit einem Speichermittel (**120**) versehen ist, und einen mit dem Speichermittel (**120**) über einen Übertragungsbus (B1, B2) verbundenen lokalen Speicher (**210**) enthält, **gekennzeichnet durch** die folgenden Schritte:
   a) Herstellen wenigstens einer Datei (F) von Testvektoren,
   b) Verschlüsseln der in der Datei (F) von Testvektoren enthaltenen Daten mit Hilfe eines Verschlüsselungs-/Entschlüsselungsmittels (**10**),
   c) Installieren der verschlüsselten Datei (F') von Testvektoren im Speichermittel (**120**) der Zentraleinheit (**100**)
   d) vor jedem Test Laden der verschlüsselten Datei (F') von Testvektoren in den lokalen Speicher (**210**) über den Übertragungsbus (B1, B2),
   e) Entschlüsseln der verschlüsselten Daten der Datei (F') von Testvektoren mit Hilfe des Verschlüsselungs-/Entschlüsselungsmittels (**10**) und
   f) anschließend Ausführen des Tests.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Verschlüsselungs-/Entschlüsselungsmittel eine elektronische Chipkarte (**10**) ist, die einen geheimen Schlüssel und einen Verschlüsselungs-/Entschlüsselungs-Algorithmus enthält.
3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß nach der Entschlüsselung sensibler Daten für eine Verifikation eine Quittierungsnachricht zur Zentraleinheit (**100**) geschickt wird.
4. Verfahren nach irgendeinem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß nach dem Schritt e) der

Zugriff auf den lokalen Speicher (**210**) zum Lesen oder Modifizieren untersagt ist.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß der Zugriff auf den lokalen Speicher (**210**) zum Lesen oder Modifizieren bei Angabe einer Zugriffsberechtigung zugelassen wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß die Zugriffsberechtigung in einer elektronischen Chipkarte (**20**) enthalten ist.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 199 31 047 A1
Int. Cl.[7]: G 01 R 31/3183
Offenlegungstag: 13. Januar 2000

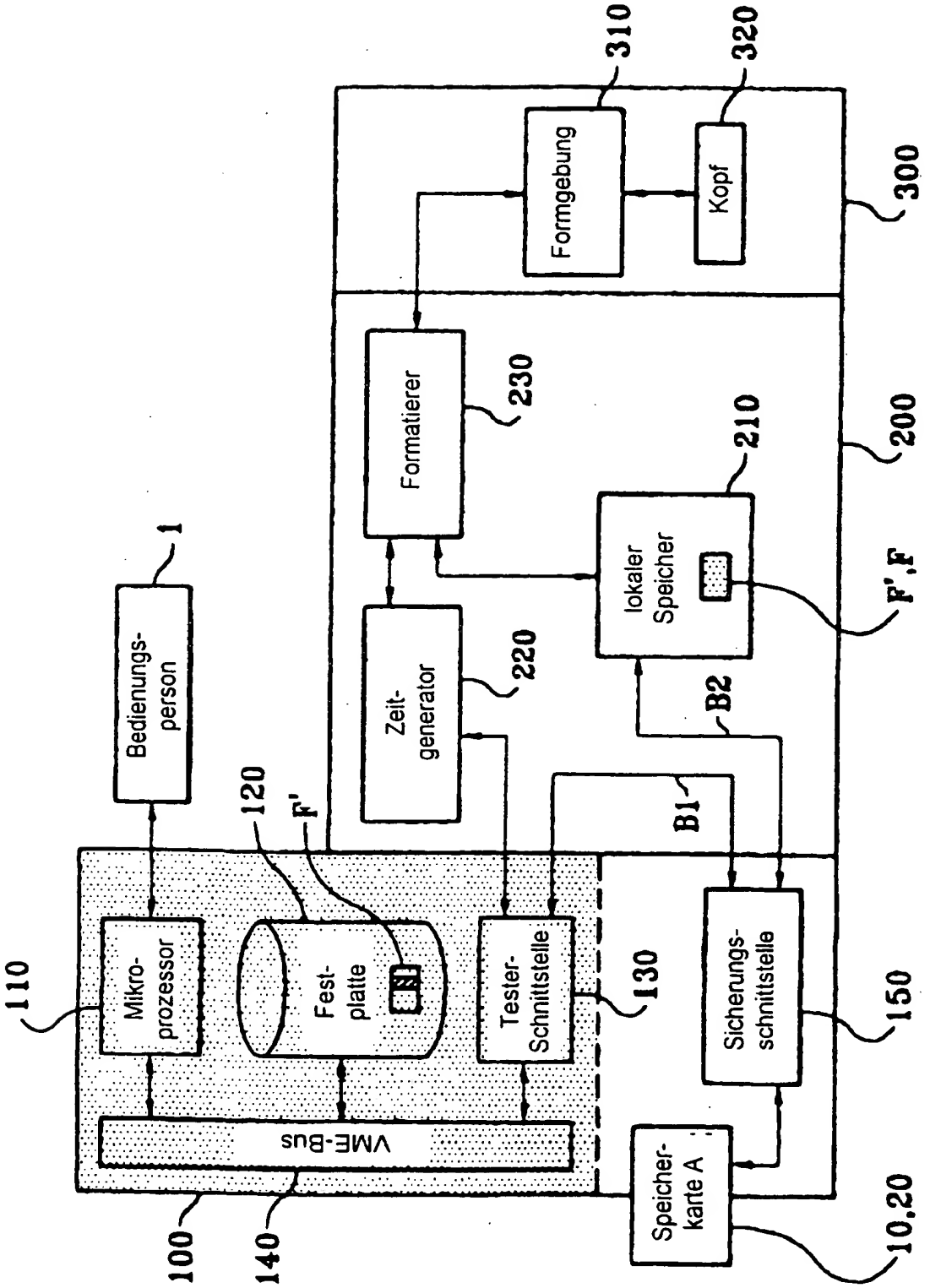


FIG.1

Nummer: DE 199 31 047 A1
Int. Cl.[7]: G 01 R 31/3183
Offenlegungstag: 13. Januar 2000

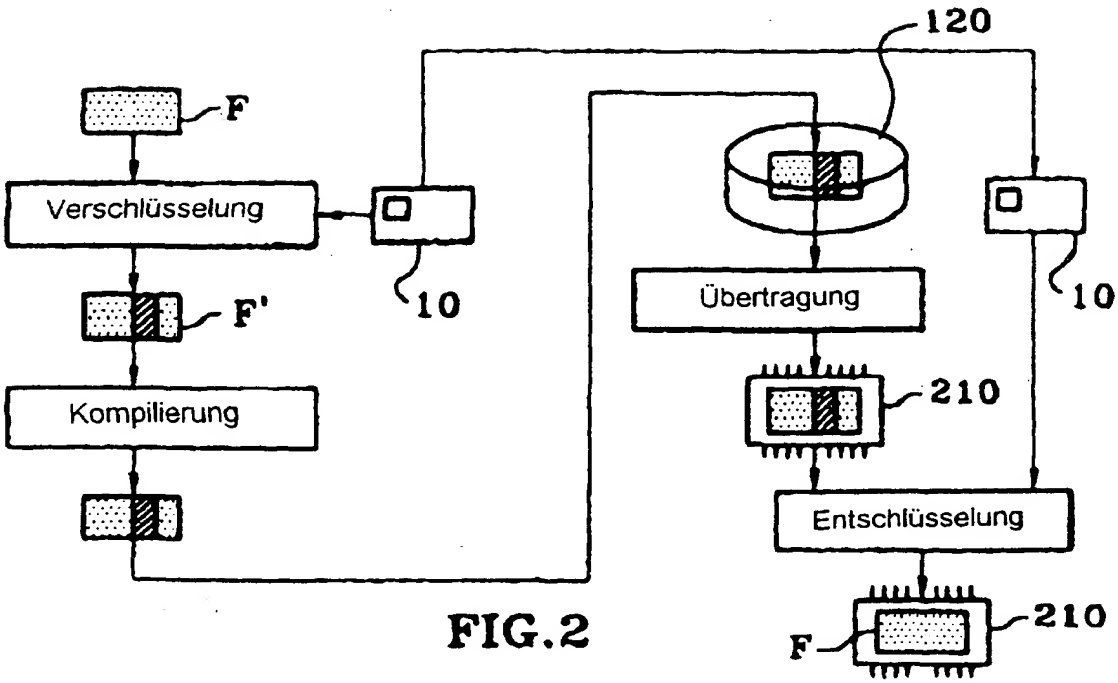


FIG.2

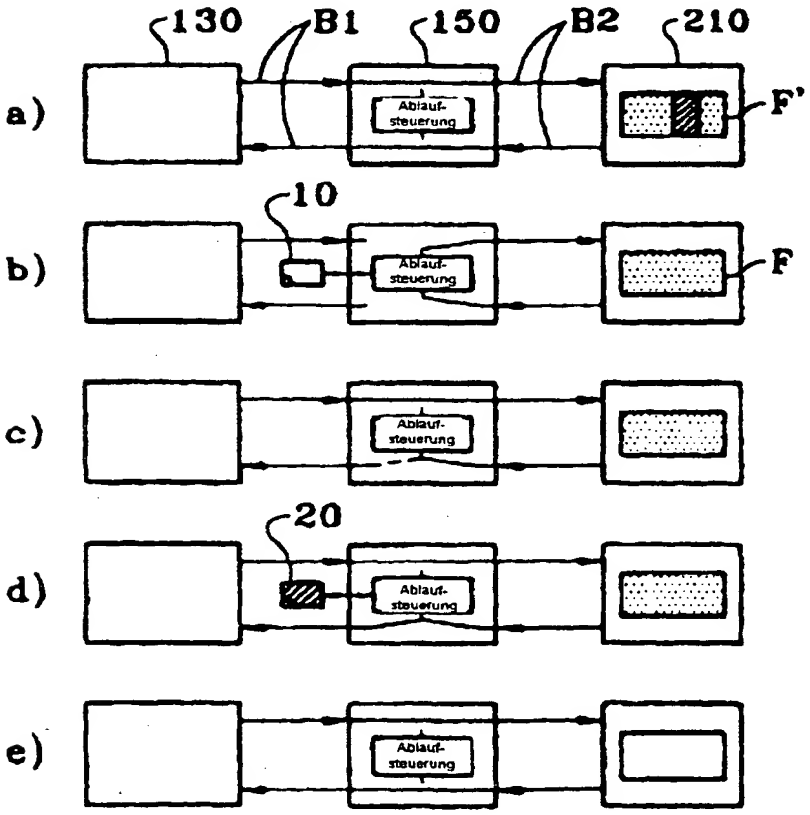


FIG.3